UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,931	07/25/2001	Robert H. Thibadeau	010321	7248

164 7590 08/05/2004

KINNEY & LANGE, P.A.
THE KINNEY & LANGE BUILDING
312 SOUTH THIRD STREET
MINNEAPOLIS, MN 55415-1002

EXAMINER	
PARTHASARATHY, PRAMILA	

ART UNIT	PAPER NUMBER
2136	12

DATE MAILED: 08/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/912,931	THIBADEAU, ROBERT H.	
	Examiner	Art Unit	
	Pramila Parthasarathy	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-136* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-136* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *#4,#6,#9,#11*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the application filed on 02/17/2004. Claims 1 – 122 were received for consideration. Preliminary amendments to the claims were filed. Claims 1 and 89 were amended. New claims 123 – 136 were added. Claims 1 – 136 are currently being considered.

2. Three initialed and dated copies of Applicant's IDS form 1449, Paper No.4, 6, 9 and 11 are attached to the Office action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1 – 15, 20 – 24, 28,29, 32 – 42, 46 – 49, 53 – 70, 75 – 78, 82, 83, 86 – 103, 108 – 112, 116, 117, 120 – 128, 130 - 136 are rejected under 35 U.S.C. 102(e) as being anticipated by Diamant et al. (Patent Number 6,268,789).

Regarding Claim 1, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), and said method comprising:

partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record (Fig. 2, 5, 8, 11, 14 and Column 5 line 25 – Column 6 line 60); and

limiting access to the security partition of said storage device by said operating system of said computer system (Fig. 8; Column 8 line 62 – Column 9 line 9; Column 10 line 54 – Column 11 line 20 and Column 12 line 1 – Column 13 line 53).

Regarding Claim 35, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), and said system for promoting security comprising:

a security partition formed in said storage device having at least one authority record and at least one data set associated with said authority record (Fig. 2, 5, 8, 11, 14 and Column 5 line 25 – Column 6 line 60); and

wherein access to said partition in said storage device by said operating system of said computer system is limited (Fig. 8; Column 8 line 62 – Column 9 line 9; Column 10 line 54 – Column 11 line 20 and Column 12 line 1 – Column 13 line 53).

Regarding Claim 56, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), said medium comprising:

instructions for partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record (Fig. 2, 5, 8, 11, 14 and Column 5 line 25 – Column 6 line 60); and

instructions for limiting access to at least a portion of said storage device by said operating system of said computer system (Fig. 8; Column 8 line 62 – Column 9 line 9; Column 10 line 54 – Column 11 line 20 and Column 12 line 1 – Column 13 line 53).

Regarding Claim 89, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and

Column 5 line 25 – Column 15 line 22), and said system for promoting security comprising:

means for partitioning at least a portion of said storage device to form a security partition having at least one authority record and at least one data set associated with said authority record (Fig. 2, 5, 8, 11, 14 and Column 5 line 25 – Column 6 line 60);; and

limiting access to the security partition of said storage device by said operating system of said computer system (Fig. 8; Column 8 line 62 – Column 9 line 9; Column 10 line 54 – Column 11 line 20 and Column 12 line 1 – Column 13 line 53).

Regarding Claim 123, Diamant teaches and describes, a storage device for promoting security in a computer system (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), the storage device comprising:

a storage medium for storing data (Fig. 2 and Column 5 line 25 – Column 6 line 22);

firmware for reading data from and writing data to the storage medium (Column 9 line 42 – Column 10 lines 60); and

a partition defined on the storage medium for dividing the storage medium into a data partition and a secure data partition, the secure data partition for storing secure data and one or more authority records (Fig. 2, 5, 8, 11, 14 and Column 5 line 25 – Column 6 line 60);

wherein only the firmware is permitted to access the secure data and the one or more authority records (Fig. 8; Column 8 line 62 – Column 9 line 9; Column 10 line 54 – Column 11 line 20 and Column 12 line 1 – Column 13 line 53).

Regarding Claim 132, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with a storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), the method comprising:

partitioning a storage medium of the storage device into a data partition and a secure data partition, the data partition being accessible to the user and the secure data partition being invisible to the user, the secure data partition for storing secure data and one or more authority records(Fig. 2, 5, 8, 11, 14 and Column 5 line 25 – Column 6 line 60); and

the secure data and the one or more authority records (Fig. 8; Column 8 line 62 – Column 9 line 9; Column 10 line 54 – Column 11 line 20 and Column 12 line 1 – Column 13 line 53).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on

said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said computer system includes a networked computer system (Fig. 1 Column 5 lines 25 – 65).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein at least a portion of said storage device firmware comprises writeable firmware (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein at least a portion of said storage device firmware comprises non-writeable firmware (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having

an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising transporting data to said storage device only in connection with execution of said firmware of said storage device (Column 10 lines 30 – 53 and Column 14 lines 32 – 67).

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol (Column 13 lines 23 – 35).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said partitioning step occurs on a low-level formatting portion of said storage device (Column 13 line 23 – Column 14 line 67).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device (Column 7 line 43 – Column 8 line 30).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising said security partition having a master authority record (Column 6 line 9 – 54).

Claim 11 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22),

further comprising translating information from a master authority record included in said storage device to a group authority in said operating system (Column 9 line 3 – Column 10 line 29).

Claim 12 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising writing said security partition using a security partition open call (Column 5 lines 4 – 54 and Column 19 line 29 – Column 21 line 54).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising reading said security partition after a predetermined time interval (Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 20 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising encrypting at least a portion of said security partition (Column 14 line 32 – Column 15 line 4).

Claim 21 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising encrypting data on said storage device so that only an external agent can decrypt said encrypted data (Column 14 line 32 – Column 15 line 4).

Claim 22 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22),

further comprising providing no method for decrypting data stored on said storage device with information available on said storage device (Column 5 lines 4 – 24 and Column 13 line 25 – Column 14 line 68).

Claim 23 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising hiding at least one field of said authority record (Column 17 line 43 – Column 18 line 18).

Claim 24 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing a hash of code in a passcode field of said authority record (Column 13 lines 1 – 22).

Claim 28 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having

an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising declaring at least a portion of data in said security partition to be write-once (Column 1 lines 45 – 63 and Column 2 line 47 – 60).

Claim 29 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising permitting only a predetermined user to access a master authority record of said security partition (Column 6 line 9 – 54).

Claim 32 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the authority record includes at least one time value associated with processing of a portion of data stored on said storage device (Column 5 line 4 – Column 8 line 18 and Column 13 lines 1 – 22).

Claim 33 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said time value is selected from the group consisting of a start time and an end time (Column 13 lines 1 – 22 and Column 17 line 10 – Column 19 line 61).

Claim 34 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing call authentication data on said storage device (Column 6 line 41 – Column 8 line 30 and Column 9 line 42 – Column 10 line 60).

Claim 36 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line

22), wherein said computer system includes a networked computer system (Fig. 1 Column 5 lines 25 – 65).

Claim 37 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein at least a portion of said storage device firmware comprises writeable firmware (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim 38 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein at least a portion of said storage device firmware comprises writeable firmware (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim 39 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device,

wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol (Column 13 lines 23 – 35).

Claim 40 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said partitioning step occurs on a low-level formatting portion of said storage device (Column 13 line 23 – Column 14 line 67).

Claim 41 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising said security partition having a master authority record (Column 6 line 9 – 54).

Claim 46 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising encrypted data stored in on said storage device (Column 14 line 32 – Column 15 line 4).

Claim 47 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising at least one hidden field in said authority record (Column 17 line 43 – Column 18 line 18).

Claim 48 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line

22), further comprising said authority record having a passcode field (Column 13 lines 1 – 22).

Claim 49 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising a hidden key stored in said storage device (Column 17 line 43 – Column 18 line 18).

Claim 53 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the authority record includes at least one time value associated with processing of a portion of data stored on said storage device (Column 5 line 4 – Column 8 line 18 and Column 13 lines 1 – 22).

Claim 55 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing call authentication data stored on said storage device (Column 6 line 41 – Column 8 line 30 and Column 9 line 42 – Column 10 line 60).

Claim 57 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said computer system includes a networked computer system (Fig. 1 Column 5 lines 25 – 65).

Claim 58 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein at least a portion of said

storage device firmware comprises writeable firmware (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim 59 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein at least a portion of said storage device firmware comprises non-writeable firmware (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim 60 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising transporting data to said storage device only in connection with execution of said firmware of said storage device (Column 10 lines 30 – 53 and Column 14 lines 32 – 67).

Claim 61 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol (Column 13 lines 23 – 35).

Claim 62 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said partitioning step occurs on a low-level formatting portion of said storage device (Column 13 line 23 – Column 14 line 67).

Claim 63 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a

processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising adding data to said storage device in an orientation selected for promoting identification of remaining data storage space on said storage device (Column 7 line 43 – Column 8 line 30).

Claim 64 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising said security partition having a master authority record (Column 6 line 9 – 54).

Claim 65 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising said master authority record governing all said authority records in said storage device (Column 6 line 41 – Column 8 line 30).

Claim 66 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising translating information from a master authority record included in said storage device to a group authority in said operating system (Column 9 line 3 – Column 10 line 29).

Claim 67 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for writing said security partition using a security partition open call (Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 69 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a

processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for reading said security partition using a security partition open call (Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 75 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for encrypting at least a portion in said security partition (Column 14 line 32 – Column 15 line 4).

Claim 76 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for encrypting data on said storage device so that only an external agent can decrypt said encrypted data (Column 14 line 32 – Column 15 line 4).

Claim 77 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for hiding at least one field of said authority record (Column 17 line 43 – Column 18 line 18).

Claim 78 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for storing a hash of code in a passcode field of said authority record (Column 13 lines 1 – 22).

Claim 82 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a

processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for storing at least a portion of data in said security partition to be write-once (Column 1 lines 45 – 63 and Column 2 line 47 – 60).

Claim 83 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for permitting only a predetermined user to access a master authority record of said security partition (Column 6 line 9 – 54).

Claim 86 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the authority record includes at least one time value associated with processing of a portion of data stored on said storage device (Column 5 line 4 – Column 8 line 18 and Column 13 lines 1 – 22).

Claim 88 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising of instructions for storing call authentication data on said storage device (Column 6 line 41 – Column 8 line 30 and Column 9 line 42 – Column 10 line 60).

Claim 90 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said computer system includes a networked computer system (Fig. 1 Column 5 lines 25 – 65).

Claim 91 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line

22), wherein at least a portion of said storage device firmware comprises writeable firmware (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim 92 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein at least a portion of said storage device firmware comprises non-writeable firmware (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim 93 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising transporting data to said storage device only in connection with execution of said firmware of said storage device (Column 10 lines 30 – 53 and Column 14 lines 32 – 67).

Claim 94 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said storage device is configured in accordance with a protocol selected from the group consisting of ATA protocol and SCSI protocol (Column 13 lines 23 – 35).

Claim 95 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said partitioning step occurs on a low-level formatting portion of said storage device (Column 13 line 23 – Column 14 line 67).

Claim 96 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising adding data to said storage device in an orientation selected for

promoting identification of remaining data storage space on said storage device (Column 7 line 43 – Column 8 line 30).

Claim 97 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising said security partition having a master authority record (Column 6 line 9 – 54).

Claim 98 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for said master authority record to govern all said authority records in said storage device (Column 6 line 41 – Column 8 line 30).

Claim 99 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device,

wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising translating information from a master authority record included in said storage device to a group authority in said operating system (Column 9 line 3 – Column 10 line 29).

Claim 100 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for writing said security partition using a security partition open call (Column 5 lines 4 – 54 and Column 19 line 29 – Column 21 line 54).

Claim 102 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for reading said security partition using a security partition open call (Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 103 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for closing said security partition after a predetermined time interval (Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 108 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for encrypting at least a portion of said data in said security partition (Column 14 line 32 – Column 15 line 4).

Claim 109 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line

22), further comprising means for encrypting data on said storage device so that only an external agent can decrypt said encrypted data (Column 14 line 32 – Column 15 line 4).

Claim 110 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for providing no method for decrypting data stored on said storage device with information available on said storage device (Column 5 lines 4 – 24 and Column 13 line 25 – Column 14 line 68).

Claim 111 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for hiding at least one field of said authority record (Column 17 line 43 – Column 18 line 18).

Claim 112 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system

having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for storing a hash of code in a passcode field of said authority record (Column 13 lines 1 – 22).

Claim 116 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for declaring at least a portion of data in said security partition to be write-once (Column 1 lines 45 – 63 and Column 2 line 47 – 60).

Claim 117 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for permitting only a predetermined user to access a master authority record of said security partition (Column 6 line 9 – 54).

Claim 120 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the authority record includes at least one time value associated with processing of a portion of data stored on said storage device (Column 5 line 4 – Column 8 line 18 and Column 13 lines 1 – 22).

Claim 121 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said time value is selected from the group consisting of a start time and an end time (Column 13 lines 1 – 22 and Column 17 line 10 – Column 19 line 61).

Claim 122 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line

22), further comprising means for storing call authentication data on said storage device (Column 6 line 41 – Column 8 line 30 and Column 9 line 42 – Column 10 line 60).

Claim 124 is rejected as applied above in rejecting claim 123. Furthermore, Diamant teaches and describes, a storage device for promoting security in a computer system (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the one or more authority records include one master authority record (Column 6 line 9 – 54).

Claim 125 is rejected as applied above in rejecting claim 123. Furthermore, Diamant teaches and describes, a storage device for promoting security in a computer system (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the storage device is in communication with a computer system having an operating system (Fig. 4 and Column 8 line 41 – Column 9 line21).

Claim 127 is rejected as applied above in rejecting claim 123. Furthermore, Diamant teaches and describes, a storage device for promoting security in a computer system (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the one or more authority records define access permissions relating to the secure data partition and the secure data (Column 6 line 9 – 54).

Claim 130 is rejected as applied above in rejecting claim 123. Furthermore, Diamant teaches and describes, a storage device for promoting security in a computer

system (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the storage device further comprises:

cryptographic operations embedded in the firmware of the storage device (Column 10 lines 30 – 53; Column 14 lines 32 – 55 and Column 15 lines 1 – 6).

Claim 133 is rejected as applied above in rejecting claim 132. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with a storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising

prohibiting access to the secure data partition by the operating system of the computer system (Column 10 lines 30 – 60)

Claim 134 is rejected as applied above in rejecting claim 132. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with a storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein a portion of the firmware is non-writeable (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim 135 is rejected as applied above in rejecting claim 132. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with a storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising:

writing data to the secure data partition by executing a portion of the firmware of the storage device (Column 10 lines 30 – 53 and Column 14 lines 32 – 67) ; and

associating the data with a particular record of the one or more authority records (Column 6 line 9 – 54).

Claim 136 is rejected as applied above in rejecting claim 132. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with a storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the secure data is encrypted and wherein cryptographic code is embedded in the firmware, the method further comprising:

authenticating the cryptographic code with a root assurance in the storage device (Fig. 5, 8 and Column 12 line 34 – Column 13 line 13).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising said master authority record governing all said authority records in said storage device (Column 6 line 41 – Column 8 line 30).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising closing said security partition after a predetermined time interval (Column 5 lines 4 – 54 and Column 19 line 29 – Column 21 line 54).

Claim 15 is rejected as applied above in rejecting claim 14. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising closing said security partition after a predetermined time interval

(Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 42 is rejected as applied above in rejecting claim 41. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising said master authority record being in operative association with a group authority records in said operating system (Column 6 line 41 – Column 8 line 30).

Claim 54 is rejected as applied above in rejecting claim 53. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said time value is selected from the group consisting of a start time and an end time (Column 13 lines 1 – 22 and Column 17 line 10 – Column 19 line 61).

Claim 68 is rejected as applied above in rejecting claim 67. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for

promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for reading said security partition using a security partition open call (Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 70 is rejected as applied above in rejecting claim 69. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising instructions for closing said security partition after a predetermined time interval (Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 87 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said time value is selected

from the group consisting of a start time and an end time (Column 13 lines 1 – 22 and Column 17 line 10 – Column 19 line 61).

Claim 101 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for closing said security partition after a predetermined time interval (Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 103 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising means for closing said security partition after a predetermined time interval (Column 5 lines 4 – 54; Column 17 lines 10 – Column 18 line 22 and Column 19 line 29 – Column 21 line 54).

Claim 126 is rejected as applied above in rejecting claim 125. Furthermore, Diamant teaches and describes, a storage device for promoting security in a computer system (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein secure data stored in the secure data partition is invisible to the operating system (Column 17 line 43 – Column 18 line 18).

Claim 128 is rejected as applied above in rejecting claim 123. Furthermore, Diamant teaches and describes, a storage device for promoting security in a computer system (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein the secure data is accessed by the firmware using a security partition open call internal to the storage device and hidden from a user (Column 17 line 43 – Column 18 line 18).

Claim 131 is rejected as applied above in rejecting claim 130. Furthermore, Diamant teaches and describes, a storage device for promoting security in a computer system (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein at least a portion of said storage device firmware comprises non-writeable firmware (Column 10 lines 30 – 53 and Column 14 lines 32 – 55).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 16 – 19, 25 –27, 30, 31, 43 – 45, 50 – 52, 71 – 74, 79 – 81, 84, 85, 104 – 107, 113 – 115, 118, 119, and 129 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diamant et al. (Patent Number: 6,268,789 herein after "Diamant") in view of Aucsmith et al. (Patent Number: 5,940,513 herein after Aucsmith).

Claim 16 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a public-private pair. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line

22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a public-private key as taught by Aucsmith for authenticating data originating from said security partition as taught by Diamant. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing public-private key.

Claim 18 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing a symmetric key on said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a symmetric key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a symmetric key

(Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for storing a symmetric key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by storing symmetric key.

Claim 19 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising using a private key for decoding a passcode transmitted to said authority record of said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose using a private key for decoding a passcode transmitted to said authority record of said storage device. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said using a private key in storage device (Aucsmith Fig. 4 – 6, and Column 4

line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for using a private key for decoding a passcode in storage device as taught by Aucsmith for authenticating data using a key in the security partition as taught by Diamant. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by using a private key for decoding a passcode transmitted to said authority record of said storage device.

Claim 25 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key(Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a symmetric key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and

Column 5 line 25 – Column 15 line 22), wherein said authority record includes a symmetric key to encrypted with a public key and hiding the private key in said authority record (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for storing a symmetric key encrypted using a public key and hiding a private key as taught by Aucsmith and authenticating data originating from said security partition as taught by Diamant. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by storing symmetric key.

Claim 26 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one public key in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a public key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5

line 25 – Column 15 line 22), wherein said authority record includes a public key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a public key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing a public key.

Claim 27 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one private key is stored in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a private key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record

includes a private key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a private key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing a private key.

Claim 30 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes at least one nonce (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the authority record includes at least one nonce. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes at least one nonce for authenticating data originating from said security

partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for authority record having at least one nonce as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing at least one nonce in the authority record.

Claim 43 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a public-private pair. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6,

and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a public-private key as taught by Aucsmith for authenticating data originating from said security partition as taught by Diamant. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing public-private key.

Claim 45 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing a symmetric key on said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a symmetric key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a symmetric key (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to

implement the claimed invention by including a method for storing a symmetric key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by storing symmetric key.

Claim 50 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one public key in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a public key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a public key as taught by

Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing a public key.

Claim 51 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one private key is stored in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a private key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a private key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a private key as taught by Aucsmith for authenticating data originating from said security partition. Such

modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing a private key.

Claim 52 is rejected as applied above in rejecting claim 35. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one private key is stored in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a private key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a private key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a private key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of

Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing a private key.

Claim 71 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a public-private pair. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a public-private key as taught by Aucsmith for authenticating data originating from said security partition as taught by Diamant. Such modifications would have been obvious because

by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing public-private key.

Claim 73 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing a symmetric key on said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a symmetric key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a symmetric key (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for storing a symmetric key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage

device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by storing symmetric key.

Claim 74 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising using a private key for decoding a passcode transmitted to said authority record of said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose using a private key for decoding a passcode transmitted to said authority record of said storage device. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said using a private key in storage device (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for using a private key for decoding a passcode in storage device as taught by Aucsmith for authenticating data using a key in the security partition as taught by Diamant. Such modifications would

have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by using a private key for decoding a passcode transmitted to said authority record of said storage device.

Claim 79 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key(Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a symmetric key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a symmetric key to encrypted with a public key and hiding the private key in said authority record (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of

ordinary skill in the art to implement the claimed invention by including a method for storing a symmetric key encrypted using a public key and hiding a private key as taught by Aucsmith and authenticating data originating from said security partition as taught by Diamant. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by storing symmetric key.

Claim 80 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one public key in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a public key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to

implement the claimed invention by including a method for creating and storing a public key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing a public key.

Claim 81 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one private key is stored in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a private key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a private key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and

storing a private key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing a private key.

Claim 84 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes at least one nonce (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the authority record includes at least one nonce. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes at least one nonce for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for authority record having at least one nonce as taught by Aucsmith for authenticating data originating from

said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing at least one nonce in the authority record.

Claim 104 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a public-private pair. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a public-private key as taught by Aucsmith for authenticating data originating from said security partition as taught by Diamant. Such

modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing public-private key.

Claim 106 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing a symmetric key on said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a symmetric key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a symmetric key (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for storing a symmetric key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the

computer to selected storage areas and communication networks while providing authentication of data by storing symmetric key.

Claim 107 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising using a private key for decoding a passcode transmitted to said authority record of said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose using a private key for decoding a passcode transmitted to said authority record of said storage device. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said using a private key in storage device (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for using a private key for decoding a passcode in storage device as taught by Aucsmith for authenticating data using a key in the security partition as taught by Diamant. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and

from the computer to selected storage areas and communication networks while providing authentication of data by using a private key for decoding a passcode transmitted to said authority record of said storage device.

Claim 113 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising securing a symmetric key by encrypting said symmetric key with a public key of said authority record, and hiding a private key in said authority record, thereby permitting only said hidden private key to decode said symmetric key(Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a symmetric key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a symmetric key to encrypted with a public key and hiding the private key in said authority record (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for storing a symmetric key encrypted using a public key and hiding a private key as taught by Aucsmith and

authenticating data originating from said security partition as taught by Diamant. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by storing symmetric key.

Claim 114 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one public key in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a public key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a public key as taught by Aucsmith for authenticating data originating from said security partition. Such

modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing a public key.

Claim 115 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one private key is stored in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a private key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a private key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a private key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of

Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing a private key.

Claim 118 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising storing at least one private key is stored in said storage device (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a private key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a private key for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a private key as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the

computer to selected storage areas and communication networks while providing authentication of data by creating and storing a private key.

Claim 129 is rejected as applied above in rejecting claim 123. Furthermore, Diamant teaches and describes, a storage device for promoting security in a computer system (Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the key is a public-private pair. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a public-private key pair for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for creating and storing a public-private key as taught by Aucsmith for authenticating data originating from said security partition as taught by Diamant. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing authentication of data by creating and storing public-private key.

Claim 17 is rejected as applied above in rejecting claim 16. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data (Diamante column 5 lines 17 – 24 and Aucsmith Column 5 lines 10 – 55).

Claim 31 is rejected as applied above in rejecting claim 1. Furthermore, Diamant teaches and describes, a method for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising encrypting said nonce with a public key (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose encrypting said nonce with a public key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising encrypting said nonce with a public key (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would

have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for authority record having encrypting said nonce as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks.

Claim 44 is rejected as applied above in rejecting claim 43. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data (Diamante column 5 lines 17 – 24 and Aucsmith Column 5 lines 10 – 55).

Claim 72 is rejected as applied above in rejecting claim 71. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a

processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data (Diamante column 5 lines 17 – 24 and Aucsmith Column 5 lines 10 – 55).

Claim 85 is rejected as applied above in rejecting claim 56. Furthermore, Diamant teaches and describes, a computer-readable medium containing instruction for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising encrypting said nonce with a public key (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose encrypting said nonce with a public key. However, Aucsmith discloses a method for promoting security through access control in a computer system having an operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), further comprising encrypting said nonce with a public key (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for authority record having encrypting said nonce as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would

have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks.

Claim 105 is rejected as applied above in rejecting claim 104. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes a second public-private key pair for ensuring data can only be sent to said security partition and no other location for storing said data (Diamante column 5 lines 17 – 24; Aucsmith Column 5 lines 10 – 55).

Claim 119 is rejected as applied above in rejecting claim 89. Furthermore, Diamant teaches and describes, a system for promoting security in a computer system having an operating system in operative connection with at least one storage device, wherein said storage device includes a processor and firmware for processing data stored on said storage device (Diamant Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes at least one nonce (Diamant Fig. 8 Column 12 line 33 – Column 13 line 22). Diamant does not explicitly disclose that the authority record includes at least one nonce. However, Aucsmith discloses a method for promoting security through access control in a computer system having an

operating system in operative connection with at least one storage device (Aucsmith Fig. 1 – 8, 11, 14 and Column 5 line 25 – Column 15 line 22), wherein said authority record includes at least one nonce for authenticating data originating from said security partition (Aucsmith Fig. 4 – 6, and Column 4 line 37 – Column 5 line 25). Therefore, it would have been obvious to a person of ordinary skill in the art to implement the claimed invention by including a method for authority record having at least one nonce as taught by Aucsmith for authenticating data originating from said security partition. Such modifications would have been obvious because by combining the teachings of Aucsmith with Diamant, the secure storage device provides access to and from the computer to selected storage areas and communication networks while providing at least one nonce in the authority record.

Conclusion

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks, Washington, D.C. 20231 **or faxed to:** (703) 872-9306 for all formal communications.

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA, Fourth Floor (Receptionist).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 703-305-8912. The examiner can normally be reached on 8:00a.m. To 5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Pramila Parthasarathy
Patent Examiner
703-305-8912
July 23, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100